Cyber Claims Scenarios: What have we paid lately

CHUBB®

Type of Claim	Details of Incident
Unauthorised Access	Our Insured is a professional organisation that has an online portal for its members to access data. The organisation experienced a security incident and its service representatives noticed member registration information had been scrambled in a number of instances. An incident response manager and an IT forensics firm from our panel were engaged and it was determined that unauthorised access occurred on one of the Insured's servers. In turn, approximately USD 80,000 in incident response costs were incurred remediating this matter.
Business Interruption	Our Insured was the victim of a denial of service attack which caused a 22-hour outage to the company's website and a continued degradation of service for an additional 4 days. The incident resulted in the company's inability to sell subscriptions to customers through its website. As a result, the losses totalled USD 750,000 in business interruption losses and an additional USD 40,000 of forensic accounting service costs.

Type of Claim	Details of Incident
Ransomware	An assisted living facility experienced a "brute force" ransomware attack and a ransom of approximately USD 30,000 was demanded. After paying a small amount of the ransom demand to obtain a sampling of the decryption tool, the Insured decided to instead rely on its backups to restore its systems. While no Personally Identifiable Information was compromised as a result of the attack, several of the facility's critical systems became inoperable, including call button, security systems and its medicine tracking software. The Insured incurred losses of more than USD 250,000 to get the affected systems back on-line and an additional USD 50,000 for incident response and IT forensics services.
Ransomware	A hospital's computer system was the subject of a ransomware attack. While the attacker sought only USD 500, the Insured was unable to bill health insurance carriers, process its payroll or produce images from MRIs and CT scans. As a workaround the hospital reverted entirely to paper mode through the recovery. As a result of the attack, more than USD 700,000 was incurred for IT forensics, data recovery, business interruption and crisis management costs.
Vendor / Supply Chain	A business associate of the Insured fell victim to a ransomware attack, putting the insured's customers' personal health information at risk. The Insured consulted with an incident response manager from our panel to assess its legal obligations. The incident response manager eventually determined that there was no exfiltration of data from the business associate's system. As a result of the incident, approximately USD 20,000 in incident response costs were incurred.

Contact Us

For more information, please get in touch with us at Cyber.AP@chubb.com.

Chubb. Insured.™

Published 03/2018.